CLOUD-BASED ONLINE SOCIAL NETWORK

Auwal S. I. [1], Faisal S. I. [1], Yusuf I. M. [1], Halis Altun [1], Mustafa Kaiiali [1], A. S. Wazan [2]

[1] Department of Computer Engineering
Mevlana University, Konya, Turkey
{engrausan, faisalsishaq, idrisawaa}@ gmail.com, {haltun, mkaiiali}@mevlana.edu.tr

[2] Institute Mines-Telecom/Telecom SudParis
Paris, France
samer.wazan@telecom-sudparis.eu

ABSTRACT

Online social media network has become part of human life by transforming the way users create new social relations or relate with family and friends. Online social network (OSN) has drastically increased the rate at which people interact with each other by simplifying the means of communication. However, privacy is raising a serious concern. All user generated data within the OSN system need to be protected against unauthorized friends or hackers or even against the provider of OSN. Many research works are going on to encounter the privacy issues in OSN. This paper analyses the limitations of the recent work being done in this field and proposes an efficient abstract solution to them.

Index Terms— Cloud Computing, Online Social Network, User Privacy

1. INTRODUCTION

The use of social networking media in our societies is increasingly becoming popular. Social media networks have transformed the way people keep in touch with family, friends and the way information is disseminated across societies and around the world.

The new way of communication and information sharing attracted large users to the online social networks. The large amount of users' private data maintained by the social networks providers makes them as an attractive target for cyber-attacks [1]. This poses new risks related to users' privacy.

Twitter was a victim of successful attack in which information including user names, email addresses, session tokens and encrypted/salted password of users were compromised [2].

It is evident that OSN has problems related to privacy. Indeed, users are entrusting today their private data to multiple social networks without having guarantees on the way that their data is being held or processed. Users' privacy in online social network can be susceptible to insider attacks; for example employees of online social network can know which profiles you have visited [3]. Some OSNs may sell their users data to third party companies who can use them for commercial purposes [8]. Also government may have a direct access to users' private information through collaboration with OSN providers, as was recently revealed by one of the NSA contractors Edward Snowden [4].

Other potential breaches exist. As an example, a court order could force the OSN to reveal information [4]. Or an accidental release of private data due to a programming error may occur. Recently security bug in Facebook system causes the exposure of 6 million users' personal information to their contacts [5].

OSN can be built to explore the benefits of cloud computing paradigm where computing resources are provided as services using internet technologies to multiple users [6, 7]. This paper review many research works that have been done to mitigate these privacy issues. It also analysed their advantages and drawbacks. Then it introduces an abstract solution to the problem which is based on private cloud model.

The paper is organized as follows; section 2 discusses current related work. Section 3 presents an abstract solution to the OSN privacy issue. Section 4 concludes.

2. RELATED WORK

2.1. FlyByNight Project

FlyByNight [8], is an architecture that makes a compromise between security and usability in order to minimally affect user's workflow and retain universal accessibility.

In flyByNight, Facebook acts as a broker between application providers and end users. It is still used to maintain social network friend relationship while a Facebook API is used for key management.

All private information transmitted through Facebook is encrypted/decrypted in the client side. Users generate public/private key pair. The private key is encrypted with password and stored in the keys database in flyByNight server. Facebook does not store any private key parameters.

The architecture uses public key cryptography for one-to-one communication while proxy cryptography handles one-to-many communication in order to reduce the client side computation and storage requirement.

In one-to-one communication a private message is encrypted with the recipient public key then tagged with his ID number. Facebook passes the encrypted message to be stored in flyByNight server.

While in one-to-many communication, a Proxy Encryption technique is used. The user has to create a group associated with a key pair. To add a friend to the group, user creates a new key pair and a proxy key for this friend.

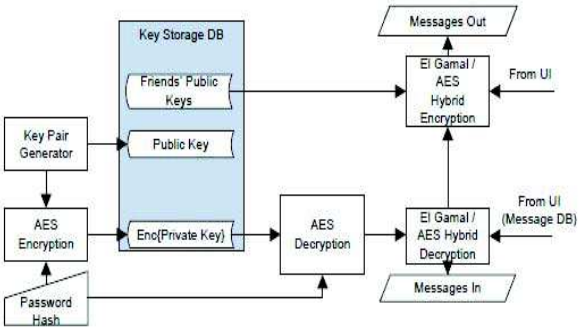

Fig. 1 flyByNight Architecture [8].

The proxy key is stored in flyByNight while the key pair is sent securely to this friend. Once the user wants to publish a message to a group of friends, he has to encrypt the message using the group public key and stores the encrypted message in flyByNight server. If a friend in the group want to read this message, he asks flyByNight to transform it to a new message encrypted using his own public key with the help of his proxy key.

FlyByNight has some advantages such as:

1. Accidental breach of information is less likely as messages are stored encrypted.
2. Programming bugs of facebook won't reveal the encrypted messages.
3. Facebook employees cannot view user's private information.

However, flyByNight has the following drawbacks: firstly, revoking a friend from a group requires re-computation of new key parameters which results in communication overhead. Secondly, users can communicate only with one group of friends at a time 9]. Lastly, it increases the burden over flyByNight server to transform the encrypted message to another form using proxy key.

2.2. FaceCloak Project

FaceCloak [7] is implemented as a web browser extension. It tries to ensure user privacy and maintains services and user interfaces at the same time.

When a user of a social networking site sets up FaceCloak in his/her browser, FaceCloak generates and distribute keys between this user and his/her friends.

Whenever a content publisher (i.e., a user who posts information in his/her account on the social networking site) wants to place a post, FaceCloak directs him to encrypt the post information and transmit it to a third party server over a TLS connection. At the same time, FaceCloak generates fake information and sent it to the OSN site.

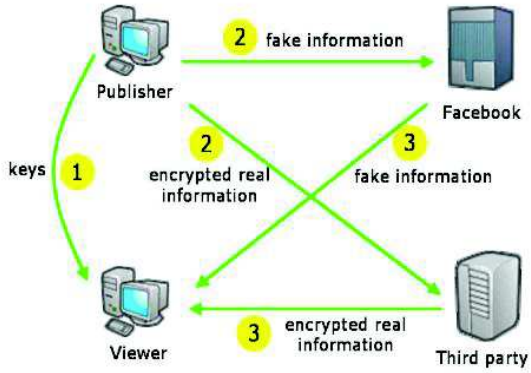

Fig. 2 FaceCloak Architecture [9]

When a content viewer (i.e., an authorized friend) wants to view the information posted. She/he decrypts the original information obtained from the third party server over a TLS connection and then replaces the fake information retrieved from the social networking site with it. This process guarantees that all OSN services will continue to work properly despite the intervention of FaceCloak.

FaceCloak has the following drawbacks:

1. FaceCloak does not have full access control mechanism as all users' friends have equal access rights to his/her information.
2. All initializing steps have to be repeated in case of adding or removing a friend. By launching timing attacks, OSNs can detect which of its users are using FaceCloak and then suspend their accounts.

2.3. NOYB Project

NOYB [10], is a mechanism that uses encryption and transformation to preserve the privacy of users' private information.

Private information of users are partitioned into multiple atoms, these atoms are grouped into classes and

stored in a dictionary. Each user has an index through which his/her atoms are linked to.

Atoms in the dictionary are then substituted with other users atoms picked pseudo randomly to provide fake data also their indexes are encrypted using symmetric key that makes it hard for an adversary to find the victim among other users.

The drawbacks of NOYB are:

1. Users have no access control in sharing their data on OSN.
2. Each time a friend is revoked, new key has to be negotiated, which results in computational complexity
3. There is no well-defined key management.

Table I compares the aforementioned approaches based parameters as Friend Revocation Cost, Access Control Support, Encryption and Trust on 3rd Party.

TABLE I
COMPARISON BETWEEN THE REVIEWED OSN APPROACHES

Approach	Friend Revocation Cost	Access Control Support	Encryption	Trust on 3rd Party
FlyByNight	High	Yes	Asymmetric	No
FaceCloak	High	Partially	Symmetric	No
NOYB	High	Partially	Symmetric	Partially

3. ABSTRACT VIEW OF THE CLOUD-BASED OSN

There are many problems associated with earlier works (as pointed out in section 2) which we tried to address in our proposed work.

In Cloud-Based OSN, the user private data (data that the social media network user wants to share with his/her friends and family) will be stored in a trusted personal cloud storage which is accessible over the internet. This may be as simple as hard disk partition on a personal laptop or a lun allocated in a trusted private cloud of an organization. This eliminates the need for encryption and reduces the computational overhead.

The OSN will serve as a friend's management portal, where friends and groups are created and managed.

When a user uploads new data to his personal cloud storage, the data management portal calls the OSN-Cloud interface to fetch his list of OSN friends/groups. A popup menu will then appear to the user to select who is allowed to access the data.

When a friend wants to access this user's published data. He has to approaches the OSN to obtain a security token which will certify him as legitimate friend of this user. Then he has to introduce this token to the OSN-Cloud interface, along with a pre-shared secret with the user. This secret is unknown to the OSN, thus the threat of OSN accessing the data by self-generating a security token is eliminated.

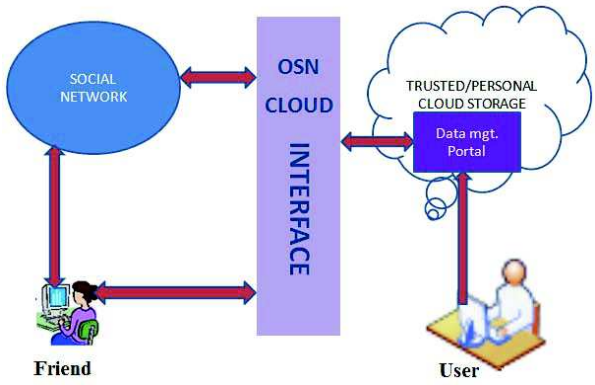

Fig.3 Cloud-Based OSN

Then the OSN-Cloud interface will establish an SSL session with that friend and enable access to the data accordingly. The access control is implemented in the data management portal side. After a friend is authenticated, the interface will fetch list of all files that he is authorized to access. He then selects the required file from the list.

Work is in progress to implement the OSN-Cloud interface and the data management portal. This can be achieved by implementing a Facebook API which is capable of communicating with external cloud storage. Table II gives the analysis parameters of our approach. As far as we are using a personal cloud storage, Encryption is not required. It will be needed in case we use a 3rd party cloud storage which we do not trust.

TABLE II
CLOUD-BASED OSN ANALYSIS PARAMETERS

	Friend Revocation Cost	Access Control Support	Encryption	Trust on 3rd Party
Cloud-Based OSN	Low	Yes	No	No

4. CONCLUSION

A lot of researches have been done in order to control the privacy risk in online social media network. Though the threat of privacy issue has been greatly undermined, some privacy and security risks still exist.

In this paper we have analysed the recent works being done to solve the privacy issues in OSNs. We have shown the advantages and limitations of each one. Finally we have presented an abstract solution to encounter these limitations.

In this work all private data are shielded from OSN and unauthorized users by storing data in trusted/personal cloud storage. Furthermore we brought a simplified means of accessing data through providing a user with token and

secret information without the need of encryption to avoid computational complexity. We believed our work when implemented would solve many privacy issues relevant to social media network.

5. REFERENCES

[1] T. N. Jagatic, N. A. Johnson, M. Jakobsson and F. Menczer, "Social phishing", Communications of the ACM, 50(10): 94-100, 2007.

[2] "Twitter hacked, 250,000 users affected", Zdnet, Feb, 2013, http://www.zdnet.com/twitter-hacked-250000-users-affected-7000010712.

[3] Nick Douglas, "Facebook Employees Know Whose Profiles You Look At", Valleywag, Oct, 2007, http://gawker.com/315901/facebook-employees-know-what-profiles-you-look-at.

[4] MATT APUZZO, "What is the problem with prism?", June, 2013, http://news.yahoo.com/whats-problem-prism-203441280.html.

[5] "Facebook Bug Exposed Email Addresses, Phone Numbers Of Million Users", http://www.huffingtonpost.com/2013/06/21/facebook-bug_n_3480739.html

[6] Buyya, Rajkumar, Christian Vecchiola, and S. Thamarai Selvi, "Mastering Cloud Computing: Foundations and Applications Programming", Access Online via Elsevier, 2013

[7] Jansen, Wayne, and Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST special publication, 2011, pp. 800-144.

[8] Lucas MM, and Borisov N., "FlyByNight: mitigating the privacy risks of social networking", the 7th ACM Workshop on Privacy in the Electronic Society (WPES'08), 2008, pp. 1–8.

[9] wanying luo, qi xie, and urs hengartner, "facecloak: an architecture for user privacy on social networking sites", IEEE International Conference on Privacy, Security, Risk and Trust (passat-09), vancouver, canada, 2009, pp. 26–33.

[10] Saikat Guha, Kevin Tang, and Paul Francis, "NOYB: privacy in online social networks", 1st Workshop on Online Social Networks (WOSP'08), 2008, pp. 210–230.